



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-333659

(P2003-333659A)

(43) 公開日 平成15年11月21日 (2003. 11. 21)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード\* (参考)

H 0 4 Q 7/38

G 0 6 F 15/00

3 3 0 C 5 B 0 8 5

G 0 6 F 15/00

3 3 0

H 0 4 B 7/26

1 0 9 R 5 K 0 6 7

H 0 4 Q 7/20

1 0 9 M

H 0 4 Q 7/04

Z

審査請求 未請求 請求項の数 7 O L (全 13 頁)

(21) 出願番号 特願2002-139058 (P2002-139058)

(22) 出願日 平成14年5月14日 (2002. 5. 14)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 前田 健司

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100076428

弁理士 大塚 康徳 (外3名)

Fターム(参考) 5B085 AE03 AE04 BA06 BG02

5K067 AA21 AA32 BB04 BB21 DD11

DD17 DD52 EE02 EE10 EE16

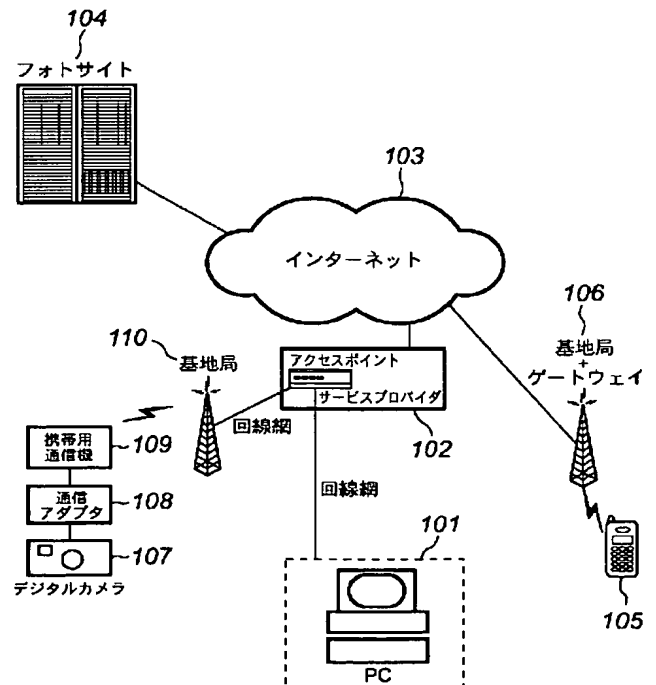
FF02 FF23 HH22 HH24

(54) 【発明の名称】 通信制御装置及び方法

(57) 【要約】 (修正有)

【課題】 イメージデバイス、アダプタ、携帯電話の組合せでイメージサービスをネットワークから受けるシステムにおいて、アダプタ携帯端末の盗難、紛失等による悪用を防止する通信制御装置及び方法を提供する。

【解決手段】 通信アダプタ108は通信機109がアクセスポイント102に対して発呼するための電話番号や、ネットワークに接続するためのユーザ名およびパスワード識別情報等を記憶する記憶手段に加えて、デジタルカメラ107からその固有IDを読み取る手段をもうけ、固有IDを呼んだ時、記憶した情報と比較し、一致したときのみネットワークへのアクセスを許可する。さらに、一致しなければ、ユーザ名およびパスワードの記憶をし直させる。



**【特許請求の範囲】**

【請求項 1】 周辺装置をネットワークに接続する通信制御装置であって、

周辺装置の識別子を取得して記憶する第 1 の記憶手段と、

ネットワークに接続するためのあて先及びパスワードを含む接続情報を記憶する第 2 の記憶手段と、

ネットワークへと接続する際に、接続された周辺装置の識別子が前記第 1 の記憶手段に記憶された識別子と一致しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第 1 の記憶手段に記憶された識別子との照合と、前記第 2 の記憶手段に記憶された前記接続情報の更新とを行わせることを特徴とする通信制御装置。

【請求項 2】 前記ネットワークへの接続時には、前記接続情報に加えて、前記周辺装置の識別子と当該通信制御装置自身の識別子とについて、前記ネットワーク上のサーバによる認証を受けることを特徴とする請求項 1 記載の通信制御装置。

【請求項 3】 前記周辺装置はイメージデバイスであることを特徴とする請求項 1 記載の通信制御装置。

【請求項 4】 前記識別子はイメージデバイスの製造番号であることを特徴とする請求項 3 記載の通信制御装置。

【請求項 5】 前記接続情報は、前記ネットワークに接続された情報処理装置から受信し、前記第 2 の記憶手段に記憶されることを特徴とする請求項 1 記載の通信制御装置。

【請求項 6】 コンピュータを、周辺装置の識別子を取得して記憶する第 1 の記憶手段と、ネットワークに接続するためのあて先及びパスワードを含む接続情報を記憶する第 2 の記憶手段として機能させると共に、

ネットワークへと接続する際に、接続された周辺装置の識別子が前記第 1 の記憶手段に記憶された識別子と一致しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第 1 の記憶手段に記憶された識別子との照合と、前記第 2 の記憶手段に記憶された前記接続情報の更新とを行わせるよう機能させることを特徴とするプログラム。

【請求項 7】 周辺装置をネットワークに接続するための通信制御方法であって、周辺装置の識別子を取得して第 1 の記憶手段により記憶する工程と、

ネットワークに接続するためのあて先及びパスワードを含む接続情報を第 2 の記憶手段により記憶する工程と、ネットワークへと接続する際に、接続された周辺装置の識別子が前記第 1 の記憶手段に記憶された識別子と一致

しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第 1 の記憶手段に記憶された識別子との照合と、前記第 2 の記憶手段に記憶された前記接続情報の更新とを行わせることを特徴とする通信制御方法。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、例えば、端末装置を通信回線を介してサーバに接続する際等に、端末装置を通信装置に接続するために用いられる通信制御装置および方法に関する。

**【0002】**

【従来の技術】従来、デジタルカメラで撮影したデジタル画像データ（以下、単に画像データと呼ぶ）は、利用者が利用者自身の有するパーソナルコンピュータ等に、シリアル通信や USB 等の通信により、あるいは、規格化されたメモリ媒体を介して移され、そこで印刷されたり、あるいはフレキシブルディスク等の媒体を介してさらに出力サービス店に持ち込まれ、画像として固定されるのが一般的である。

【0003】これに対して、画像データの加工や出力等、画像データに関する様々なサービスを提供するサーバをインターネット上に設け、デジタルカメラで撮影した画像データをサーバにより受信して、利用者にそれらサービスを提供するシステムが提案されている。このようなシステムにおいては、携帯電話機や携帯型データ通信装置等の携帯用通信機を利用することで、デジタルカメラに格納された画像データをそのままサーバに送信することもできる。

【0004】この場合、デジタルカメラと携帯用通信機とを通信アダプタを介して接続し、利用者が通信アダプタを操作することによりデジタルカメラで撮影した画像データは、通信アダプタと携帯用通信機を介してサーバへアップロードされる。サーバは画像データに対し保存だけでなく、加工、消去、移動の処理も行う。これらサーバが行う処理を携帯電話と通信アダプタからそれぞれ指示できるシステムもある。

【0005】ここで使用される通信アダプタには、表示能力の高い LCD や操作性の良いキーボード等のユーザインターフェースはなく、ネットワーク接続するための電話番号やサーバのログイン情報などを予め保存している。サーバへの接続やサービスに対する課金は、通常通信アダプタに保存された情報に基づいて行われる。

【0006】このようなシステムにおいて、通信アダプタとデジタルカメラ、携帯用通信機は、互いにケーブルやコネクタで接続されているため、移動に際しては分離して持ち運ぶ事が多い。このため、個々の機器の紛失や盗難のおそれが避けられないが、そのなかでも通信アダプタを紛失したり、盗難にあった場合には、通信アダプタ内にある情報を保護する工夫がなされていないのが実

情である。したがって、他人の通信アダプタを入手した第三者が、通信アダプタ内の情報を利用してサーバに接続し、サービスを受けることができるという問題がある。

【0007】このような問題に対する携帯端末装置のセキュリティ技術の一例として、例えば特開2000-253457号では、PHSなどの携帯機器内にある個人情報保護方法を開示している。具体的には、情報記憶部を備えた端末において、他の無線局から情報保護要求が入力された際、要求に基づき記憶部のアクセス制限や所定のデータ消去を行うことにより、機密性を実現している。

【0008】一方、特開2000-286957号では、ユーザ機器側にて簡便な方法により不正使用の危険を低減することのできる情報処理装置を開示している。この技術では、電話番号の登録手段を携帯情報端末に設け、携帯電話機と携帯情報端末とをケーブルにより通信接続して通信機能を利用するシステムにおいて、通信開始時等に、携帯情報端末が携帯電話機の電話番号を読み出し、それが登録済みの電話番号と一致する場合にのみ通信機能を利用可能とする。また、一致しない場合には携帯電話機から読み出した電話番号を秘密裡に他所に送信する技術に関して開示している。

【0009】

【発明が解決しようとする課題】しかしながら前者の方法では、権限のある、本来登録されている利用者（以下、正当利用者と呼ぶ）は、携帯機器の紛失や盗難に気づかない限りアクセス制限やデータ消去等の対応を行うことができない。そのため、アクセス制限やデータ消去等の対応を行うまでは、不正利用者による機器の不正利用を防止することができない。

【0010】また、後者の方法では、不正利用者が同じサービスの利用者であれば、そのサーバにアクセスするための電話番号を不正利用者自身の携帯電話機に登録していることも十分にあり得るため、そのような不正利用者による不正利用を防止することは困難である。

【0011】本発明は上記従来例に鑑みて成されたもので、情報の安全性をより一層向上させた通信アダプタ装置及びその制御方法を提供することを目的とする。

【0012】より具体的には、従来実現されていたセキュリティ技術では防止できなかった、正当利用者が気づかない間の不正利用の防止、および、同一サービスの利用者による不正利用の防止を、いずれも効果的に実現できる通信制御装置及び方法を提供することを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するために本発明は次のような構成を有する。

【0014】周辺装置をネットワークに接続する通信制御装置であって、周辺装置の識別子を取得して記憶する

第1の記憶手段と、ネットワークに接続するためのあて先及びパスワードを含む接続情報を記憶する第2の記憶手段と、ネットワークへと接続する際に、接続された周辺装置の識別子が前記第1の記憶手段に記憶された識別子と一致しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第1の記憶手段に記憶された識別子との照合と、前記第2の記憶手段に記憶された前記接続情報の更新とを行わせる。

【0015】この構成により、接続された周辺装置の識別子が前記第1の記憶手段に記憶された識別子と一致しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第1の記憶手段に記憶された識別子との照合と、前記第2の記憶手段に記憶された前記接続情報の更新とを行わせることで、正当利用者以外による当該通信制御装置の利用を困難ならしめ、ネットワークサービス等の不正利用を避けることができる。

【0016】さらに好ましくは、前記ネットワークへの接続時には、前記接続情報に加えて、前記周辺装置の識別子と当該通信制御装置自身の識別子とについて、前記ネットワーク上のサーバによる認証を受ける。

【0017】この構成により、ネットワークへの接続時に必要とされる、接続された周辺装置の識別子が第1の記憶手段により記憶されていない場合には、改めてその照合を行う必要があるために、周辺装置が正当利用者のものでない限り、ネットワークへの不正な接続を制限できる。

【0018】さらに好ましくは、前記周辺装置はイメージデバイスである。

【0019】この構成により、デジタルカメラ等のイメージデバイスによるネットワークサービスについて、不正利用を防止できる。

【0020】さらに好ましくは、前記識別子はイメージデバイスの製造番号である。

【0021】この構成により、デジタルカメラ等のイメージデバイスに固有かつ変更不可能な製造番号によりネットワーク接続を制限でき、より不正利用の防止を効果的に行える。

【0022】さらに好ましくは、前記接続情報は、前記ネットワークに接続された情報処理装置から受信し、前記第2の記憶手段に記憶される。

【0023】この構成により、接続情報は、ネットワークに接続された情報処理装置から受信する必要があるために、不正利用の防止をより効果的に行える。

【0024】

【発明の実施の形態】〔第1の実施形態〕本発明の実施形態を、図面を参照して説明する。

【0025】＜システム構成＞図1は、本発明の実施形態を示すシステム構成図である。

【0026】このシステムは、文字情報や画像データの送受信や表示が可能なPC（パーソナルコンピュータ）101、PC101と回線網で繋がるアクセスポイント102、アクセスポイント102とインターネット103を通じて接続するフォトサイト（サーバと称す）104、サーバ104とデータを送受信できサーバ104に対する操作指示を設定できる端末（ここではWebブラウザ付き携帯電話で説明し、携帯電話と称す）105、サーバ104と携帯電話105を中継しプロトコル変換を行うゲートウェイ106、外部装置と接続可能なデジタルカメラ107、外部装置と接続あるいは外部装置に装着可能な携帯用通信機109、デジタルカメラ107と携帯用通信機109を接続しサーバ104との通信を制御する通信アダプタ108、携帯用通信機109とアクセスポイント102を中継する基地局110で構成される。

【0027】デジタルカメラ107が外部装置と接続するためのインターフェースにはUSB（ユニバーサルシリアルバス）などがある。また、携帯用通信機109は、例えばCF（コンパクトフラッシュ（登録商標））カード型のPHS（簡易型携帯電話：パーソナルハンディフォンシステム）通信デバイスなどがある。また、通信アダプタ108としては、例えば前述したCFカード型の通信デバイスを装着可能な個人情報端末などを利用できる。

【0028】ユーザはサーバ104に対しPC101を通じてユーザ登録を行う。ユーザ登録では、ユーザ名（User ID）、パスワード（User Password）、ユーザが使用する携帯電話105の電話番号（携帯電話番号：User Tel Number）、通信アダプタ108の識別子（アダプタ識別子：Adapter ID）、カメラ107の識別子（カメラ識別子：Camera ID）、通信アダプタ108と接続する携帯用通信機109の電話番号（アダプタ電話番号：Adapter Tel Number）の登録を行う。アダプタ識別子およびカメラ識別子としては、例えばそれら機器の製造時に割り当てられた番号や、あるいは利用者が適当に割り当てた文字列等を利用できる。これらに加えて、サーバ104には、PC101により、サーバ104が提供する機能を利用するために用意されたアプリケーションプログラムの識別子を登録しても良い。

【0029】これらカメラ107の識別子および通信アダプタ108の識別子、あるいはそれらに加えてPC101のアプリケーションプログラムの識別子は、後述するように、通信アダプタ108自身に書き込まれて、読み出し可能に保持する。

【0030】通信アダプタ108はデジタルカメラ107と携帯用通信機109とを接続する。通信アダプタ108を利用者が操作することにより、デジタルカメラ107で撮影した画像データは通信アダプタ108と携帯

用通信機109とを介してサーバ104へアップロードされる。もちろん、サーバ104への画像データのアップロードはPC101からも行える。サーバ104は画像データに対し、その保存だけでなく、その加工、消去、移動等の処理も行う。これらサーバ104が行う処理は、携帯電話105と通信アダプタ108からそれぞれ指示できる。

【0031】＜提供されるサービス＞本システムでは、サーバ104は、サーバ104に対する携帯電話105からのログイン要求と、通信アダプタ108からのログイン要求それぞれに対して認証を行うログインサービスを行う。なお、通信アダプタ108からのログイン情報には、デジタルカメラ107により与えられる情報を含むことから、これをデジタルカメラ107と通信アダプタ108との組み合わせからのログインということもできる。

【0032】ログイン要求するとき携帯電話105はサーバ104に対してユーザ名とパスワードとを送信する。一方、通信アダプタ108は、ログイン時にサーバ104に対してアダプタ識別子とカメラ識別子とを送信する。サーバ104は、携帯電話105または通信アダプタ108から送信されたログイン情報が正しいか判定して認証処理を行う。サーバ104によりログイン認証された携帯電話105とデジタルカメラ107と通信アダプタ108の組合せは、それぞれサーバに対し処理コマンドや画像データを送信することができる。サーバ104から携帯電話105と通信アダプタ108への処理コマンドや画像データの送信も可能である。

【0033】本システムは、携帯電話105とデジタルカメラ107と通信アダプタ108とサーバ104の共同動作によって実施されるサービスを提供する。しかし、共同動作によって実施されるサービスは、サービス実施時にサーバ104と携帯電話105と通信アダプタ108とデジタルカメラ107が同時に接続されている必要があるが、この条件が常時満たされているとは限らない。必要な機器がすべてサーバに接続されていないような事態に対応できるように、本システムでは、サーバ104が同期動作を管理（同期管理：Sync Control）する機能を有し、同期管理サービスを提供する。

【0034】本システムのサーバ104による同期管理処理（Sync Control）を用いたサービスの一例として、通信アダプタ108内に保持した個人情報や画像データを消去するサービスがある。このサービスを実現するために携帯電話105による消去設定をコマンド送信（Send Command）サービスで実現する。コマンド送信サービスは次の操作を行う。

【0035】携帯電話105から、通信アダプタ108が管理する情報の消去処理をサーバ104により行わせるために、携帯電話105はサーバ104に消去コマン

ド (DelAdapterInfo) を送信する。サーバ104は、消去コマンドの受信を受けて、携帯電話105による、通信アダプタ108の情報消去のための消去処理の設定として記憶しておく。消去対象は、消去コマンドのパラメータとして指定させることができる。

【0036】一方通信アダプタ108は、サーバ104にログインし、サーバ104によるログイン認証サービスで認証を受けると、サーバ104に対し同期動作要求コマンド (Sync) を送信する。サーバ104は同期動作要求コマンド (Sync) を受信することで同期制御処理 (SyncControl) を実行する。サーバ104は、携帯電話105による消去処理の設定が完了していれば、同期動作処理のもとで通信アダプタ108に消去コマンド (DelAdapterInfo) を送信する。通信アダプタ108はサーバ104から消去コマンド (DelAdapterInfo) を受信すると通信アダプタ108が管理する個人情報や画像データの消去処理を行う。消去対象は、パラメータ等で指定させることもできる。なお、同期制御サービスは、両方向で行うことができる。すなわち、通信アダプタ108により、携帯電話105に対するデータの消去や更新等の同期制御処理、すなわち通信アダプタ108と携帯電話105との同期保持動作の設定をサーバ104上でい、携帯電話105のログイン後に、設定された同期制御処理を実行させることもできる。

【0037】また本システムは以下のサービスも提供する。まず、通信アダプタ108の操作によって実現されるサービスについて述べる。

【0038】通信アダプタ108の操作によりユーザがデジタルカメラ107で撮影した画像データをサーバ104内の個人データ領域に保存するデータアップロード (AddData) サービスがある。データアップロードサービスはログインサービスと同期制御サービスの後、実施される。データアップロードサービスは次の様に実行される。

【0039】通信アダプタ108は、サーバ104からの制御命令、あるいは、通信アダプタ108自身の操作を待つ。通信アダプタ108は、その操作に応じてデジタルカメラ107で撮影した画像データを制御命令によりサーバ104へアップロードすることができる。このサービスでは通信アダプタ108は、画像データのアップロード要求 (AddData) として、あるいはそれに加えて、サーバ104に対して画像ファイルのインデックスと画像データを送信する。サーバ104はこれを受信すると、その画像データを、それをアップロードしたユーザに割りあてられている個人データ領域に追加する。

【0040】次に、携帯電話105の操作によって実現されるサービスについて述べる。第1のサービスは、携帯電話105の操作によりサーバ104の個人データ領

域に保存されている画像データを閲覧できるサービスである。このサービスはログインサービスと同期制御サービスの後実施される。ユーザは、サーバ104内の画像データを閲覧するために携帯電話105のウェブブラウザ機能を用いて画像閲覧の要求をする。画像閲覧要求を受けたサーバ104は保存されている画像データを携帯電話105で閲覧可能な形式に加工する。加工の対象となる画像データはサーバ104の個人データ領域に保存されている全てのファイルであるが、画像閲覧要求時にリストなどから選択する手段があってもよい。さらに、加工された画像データを携帯電話105へ送信することで閲覧サービス (MakeThumbnail) を実施する。

【0041】また、携帯電話105の操作によってサーバ104内に保存されている画像データを消去するデータ消去 (DeleteData) サービスが実現される。データ消去サービスはログインサービスと同期制御サービスの後実施される。ユーザは携帯電話105のウェブブラウザ機能を用いてサーバ104内の画像データ一覧から画像データを選択し、選択した画像データの消去処理を要求する。サーバ104は画像データの消去処理要求 (DeleteData) を受信すると、選択された画像データをログインしている当該ユーザの個人データ領域から消去する。

【0042】上述した各種機能を提供するために、サーバ104は図2のソフトウェア構成を有する。

【0043】<サーバ104のソフトウェア構成>図2は、アプリケーションサーバ104のソフトウェアモジュール構成図である。

【0044】ブラウザフォン (1001) は、ウェブブラウジング機能を持つ携帯電話である。これはWAP (Wireless Application Protocol) におけるWSPやWTP、NTTの提供するiモードのAL/TLといった擬似HTTPプロトコルをサポートするものでも良い。

【0045】WWWサーバ (1003) は、ブラウザフォン (1001) からのHTTPプロトコルによる要求を受け、適切なデータを返す。またCGI (Common Gateway Interface) 機能により、要求に応じたプログラムを呼び出す機能を有する。

【0046】ブラウザフォンマネージャ (1004) は、WWWサーバ (1003) のCGI機能から呼び出されるプログラムからの接続を待ち受け、以下の機能を実現する。

- ・WWWサーバ (1003) に接続してきたユーザー毎のユーザー認証機能

- ・V (仮想) ブラウザフォン (1002) 生成機能。

【0047】認証モジュール (Cert:1012) は、認証リクエストを受け、ユーザDB (データベース) I/F (インターフェース) (1011) を通して

ユーザDB（1010）のレコードを参照することにより認証機能を実現する。認証リクエストは、ブラウザフォンマネージャ（1004）と、アダプタマネージャ（1019）から発行される。つまり、以下2通りの認証機能を有する。

- ・ブラウザフォンマネージャ（1004）の認証
- ・アダプタマネージャ（1019）の認証。

【0048】ユーザDB I/F（1011）は、認証モジュール（1012）と、コマンド送信モジュール（1018）からのユーザDB（1010）に対する読み出し、書き込み要求を受け取り、結果を返す。同一要素に対する同時書き込み、といったデータベース操作に対する矛盾を解決する。

【0049】ユーザDB（1010）は、ブラウザフォン（1001）とアダプタ（1020）+デジタルカメラ（1021）の認証機能のためのデータベースである。ユーザDB I/F（1011）に対してデータベースアクセス手段を提供する。また、ユーザDB（1010）は、各ユーザ毎のログイン認証のための情報や、後述する通信アダプタ使用時のアダプタ認証のためのフィールドを持つ。そのフィールドとしては、ユーザ毎に、例えば、ユーザIDやパスワード、携帯電話番号、アダプタ電話番号、アダプタ識別子、カメラ識別子等が含まれる。

【0050】Vブラウザフォン（1002）は、ブラウザフォンマネージャ（1004）により、WWWサーバ（1003）にアクセスのあったユーザー毎に生成される。ブラウザフォン（1001）と、WWWサーバ（1003）を介して通信し、ブラウザフォン（1001）からのリクエストにより以下の機能呼び出し、結果を受け取ることができる。

- ・アダプター同期動作制御機能
- ・画像インデックス作成、取得機能
- ・サーバー画像取得、削除機能
- ・アダプター画像取得、削除機能。

【0051】同期制御モジュール（1005）は、Vブラウザフォン（1002）からのコマンドにより、同期制御DB I/F（1006）を通じて同期制御DB（1007）のエントリーを書換えることで、アダプター同期動作制御機能を実現する。

【0052】同期制御DB I/F（1006）は、同期制御（1005）や同期制御エージェントサーバ（Sync Agent Server：1013）からの同期制御DB（1007）に対する読み出し、書き込み要求を受け取り、結果を返す。同一要素に対する同時書き込み、といったデータベース操作に対する矛盾を解決する。

【0053】同期制御DB（1007）は、同期制御エージェントサーバ（1013）のアダプター同期動作機能を制御するためのデータベースである。同期制御DB

I/F（1006）に対してデータベースアクセス手段を提供する。また、同期制御DB（1007）は、アダプタ識別子、及びそれに対応するジョブリストのフィールドを持つ。ジョブリストが、アダプタ識別子で特定される通信アダプタにおいて実行されるべき処理の内容を示す。

【0054】インデックス作成モジュール（Make Index：1009）は、ブラウザフォン（1001）からの要求により、サーバー上の例えばハードディスク等に確保された個人メモリ（1017）に保存した画像をブラウザフォン（1001）で表示できるように変換する機能を持つ。

【0055】MAPマネージャ（1008）は、Vブラウザフォン（1002）からのアダプタ（1020）への要求コマンドを中継する。Vブラウザフォン（1002）とV（仮想）アダプタ（1014）のリストを持つ。

【0056】アダプタ（1020）と、デジタルカメラ（1021）は、図1で示した通信アダプタ108とデジタルカメラ107にそれぞれ相当する。

【0057】アダプタマネージャ（1019）は、アダプタ（1020）の接続を受け付け、以下の機能を実現する。

・接続してきたアダプタ（1020）毎のアダプター認証機能

- ・Vアダプタ（1014）生成機能
- ・アダプター同期動作機能。

【0058】Vアダプタ（1014）は、アダプタマネージャ（1019）により、アダプタマネージャ（1019）に接続してきたアダプタ（1020）毎に生成される。アダプタ（1020）と通信し、リクエストにより以下の機能呼び出し、結果を受け取る機能を有する。

- ・サーバー画像取得、削除機能
- ・アダプター画像取得、削除機能。

【0059】データ追加削除モジュール（1015）は、Vアダプタ（1014）からのコマンドにより、メモリ I/F（1016）を通じて個人メモリ（1017）に画像データを追加、削除する機能を有する。メモリ I/F（1016）は、データ追加削除モジュール（1015）やインデックス作成モジュール（1009）からの個人メモリ（1017）に対する読み出し、書き込み要求を受け取り、結果を返す。同一要素に対する同時書き込み、といったデータベース操作に対する矛盾を解決する。

【0060】個人メモリ（1017）は、アダプタ（1020）からVアダプタ（1014）を介してアップロードされる画像データを、各アダプター毎に保存する機能を有する。メモリ I/F（1016）に対してデータベースアクセス手段を提供する。個人メモリ（101

7) の内部構造は以下のようなものである。すなわち、一般のファイルシステム同様、階層構造を持つ。ユーザID (ユーザ識別子) ノードの下にアダプタID (アダプタ識別子) の階層、その下にカメラID (カメラ識別子) ノードの階層を持ち、カメラID階層の下に、画像インデックス番号付きの画像データファイルがある。なお、上記各ユーザIDノード毎に、容量制限を加えることができる。

【0061】<サービスの具体的手順>次に、アダプタ(1020)とデジタルカメラ(1021)に対してサーバ104が提供するサービスについて説明する。

【0062】図3は、サーバ104がアダプタ(1020)とデジタルカメラ(1021)に対して提供するサービスと、その各サービスにおいて図2に示したソフトウェアモジュールの呼び出される順序を示したフローチャートである。提供されるサービスには以下がある。

- ・アダプタログインサービス
- ・アダプタ同期制御サービス
- ・アダプタデータ追加削除サービス。

【0063】以下に、図3を参照してその内容を説明する。

【0064】(アダプタログインサービス)サーバ104の各種サービスを受けるためには、サーバ104に対するログインが必要となる。アダプタログインサービスは、アダプタ(1020)とデジタルカメラ(1021)の組合せがサーバ104のサービスを受けるためのログイン処理に関するサービスである。

【0065】図3(A)に示すアダプタログインサービスでは、図2に示したソフトウェアモジュールは次の順番で呼び出される。

【0066】アダプタ(1020)とデジタルカメラ(1021)の組合せからのログインサービス要求は、アダプタマネージャ(1019)が受け取る。アダプタマネージャ処理(S1101)は、認証モジュール(1012)を呼び出し、認証処理(S1102)はユーザDBI/F(1011)を経由してユーザDB(1010)から個人情報を読み出し、認証する。

【0067】(アダプタ同期制御サービス)サーバ104では、上記アダプタログインサービスにて認証が完了した際、図3(B)に示すようにアダプタ同期制御サービスを行なう。本サービスは、同期制御DB(1007)にアダプタ(1020)とデジタルカメラ(1021)の組合せがログインした時に、予め同期制御DB(1007)に各アダプタ(1020)とデジタルカメラ(1021)の組み合わせ毎に設定した同期ジョブを実行するサービスである。

【0068】上記同期ジョブとは、以下のようなものである。

【0069】サーバ104は、ブラウザフォン(1001)、アダプタ(1020)とデジタルカメラ(102

1) 及びサーバー上のサービスが共同して動作する。

【0070】ブラウザフォン(1001)からのサーバー上のサービスへの指示によりアダプタ(1020)とデジタルカメラ(1021)を制御することが可能だが、ブラウザフォン(1001)とアダプタ(1020)とデジタルカメラ(1021)が常時サーバーに接続しているわけではない。

【0071】そこでサーバ104においては、ブラウザフォン(1001)からのサーバー上のサービスへの指示を、アダプタ(1020)とデジタルカメラ(1021)のサーバーへの接続時に解決する仕組みがある。

【0072】同期動作ジョブとは、予め設定しておいたブラウザフォン(1001)からのサーバー上のサービスへ指示でき、上記アダプタ(1020)とデジタルカメラ(1021)のサーバーへの接続時に実行されるジョブのことである。

【0073】アダプタ同期制御サービスは、図2に示したソフトウェアモジュールを次の順番で呼び出す。

【0074】アダプタ(1020)とデジタルカメラ(1021)の組合せからの同期制御サービス要求は、アダプタマネージャ(1019)が受け取る。アダプタマネージャ処理(S1101)は、同期制御エージェント(1013)を呼び出し、同期制御エージェント処理(S1103)は同期制御DBI/F(1006)を経由して同期制御DB(1007)からアダプタ(1020)とデジタルカメラ(1021)の組み合わせに対するジョブを読み出し、実行する。

【0075】(アダプタデータ追加削除サービス)本サーバーシステムでは、上記アダプタログインサービス、アダプタ同期制御サービス後、ユーザーはアダプタ(1020)を通してデジタルカメラ(1021)の画像をアップロードすることができる。

【0076】本サービスは、デジタルカメラ(1021)の画像を本サーバーシステムの個人メモリ(1017)の適切な区画に格納する機能を持つ。

【0077】図3(C)に示すアダプタデータ追加削除サービスは、図2に示したソフトウェアモジュールを次の順番で呼び出す。

【0078】アダプタ(1020)とデジタルカメラ(1021)の組合せからのデータ追加削除サービス要求は、アップロードしたい画像データと共にVアダプタ(1014)が受け取る。Vアダプタ処理(S1104)は、データ追加削除モジュール(1015)を呼び出し、データ追加削除処理(S1105)はメモリI/F(1016)を通して個人メモリ(1017)の適切な区画に画像データを格納する。

【0079】<アダプタ108の説明>次に、ネットワークシステムにおけるアダプタ108について、詳しく説明する。

【0080】図4は、上記実施例におけるアダプタ10



8の電氣的構成を示すブロック図である。本実施例では、CFカードタイプのPHSカード型通信機を使ったアプリケーションを一例として説明する。

【0081】アダプタ108は、携帯用通信機用インターフェース3101を有し、このインターフェース3101介して、携帯用通信機用109を接続することができる。このCFカードコントローラ3102を経由して、携帯用通信機用109は内部バス3103に接続する。

【0082】内部バス3103には、全体動作を制御するCPU3104と、内部の動作プログラムを記憶するとともに設定内容を記憶するFlashROM3105と、プログラム実行領域であり、送受信データの一時記憶をするRAM3106と、ユーザからの操作や、ユーザへの表示を行うユーザインタフェースである操作スイッチ3107とが接続している。

【0083】操作スイッチ3107には、電源を制御するスイッチ（図示せず）と、携帯通信端末107やデジタルカメラ107への制御を行うスイッチ（図示せず）とが備えられている。

【0084】3色やキャラクタLCDなどで構成される表示機3108は、ユーザにアダプタ108の状態を通知する。

【0085】フラッシュROM3105は、電氣的に消去・書き換えが可能なROMであり、ソフトウェアの追加変更が可能である。また、一部領域を書きかえることができ、ユーザ情報などのデータを記憶保存・書き換えが可能である。アダプタ108は、携帯用通信機109に対して発信、着信、切断等を、インターフェース3102を介して制御する。

【0086】DC/DCコンバータ3109は、アダプタ108を動作させる安定化電源である。このDC/DCコンバータ3109はコネクタを介しバッテリー3110やACアダプタ・チャージャ3111から電源の供給を受ける。

【0087】アダプタ108は、デジタルカメラ107とPC101にUSBコントローラ3112を経由して接続できる。このデジタルカメラ107とは、ホスト機能3113を経由して内部バス3103に接続する。一方、PC101とはファンクション機能部3114を経由して内部バス3103に接続する。アダプタ108は、デジタルカメラ107に対してホストとして振る舞い、USBコントローラ3112を通じて制御し、デジタルカメラ107のイメージデータやカメラ内に保存してある固有情報などを読み出し、また、書きこみもすることができる。

【0088】PC101は、アダプタに対してホストとして振る舞い、PC101内で実行するアプリケーションによりアダプタ108に固有データ等を読み出し、書きこみすることができる。

【0089】なお、USBそのものの動作については規格等で明確なので詳細な説明は省略する。

【0090】アダプタ108では、通信および主な制御をソフトウェアによって実装しているので、アダプタ108の諸機能はマイクロプロセッサ3104、ROM3105、RAM3106等によって実現される。また、携帯通信端末107との接続を確立する制御、たとえば発呼・着信・切断等の制御などが実装されている。さらにTCP/IPプロトコル、PPPやTCP/IPやFTP、HTTP等も実装されている。

【0091】アダプタ108とアプリケーションサーバとの間のアプリケーションプロトコル、初期化、USB制御等のアダプタ機能制御、TCP/IPプロトコル群を介して、通信網に対して通信を行う制御などのアプリケーションもアダプタ108では実装している。

【0092】図5は、フラッシュROM3105の内部構造示す図である。

【0093】フラッシュROM3105は4Kワードのブロックに分かれており、書きこみおよび消去をする場合にはブロックごとに行うことができる。ブロック0から30までは主プログラムに割り当てられており、ブロック31にはアダプタ固有データ、ブロック32にはユーザデータが保存されている。

【0094】アダプタ情報には、プログラムのバージョン情報、特殊設定用データダウンロードをサーバから行うときの電話番号やログイン情報、アダプタ本体の固有制御情報、アダプタのシリアル番号などがある。一方、ユーザデータには、サーバへのログイン情報、アクセスポイントなどのログイン情報や電話番号、パスワード情報などがある。

【0095】アダプタ108は、PC101と接続したときに、PC101から受信したデータによってユーザデータの書きこみを行うことができる。PC101内で実行されたアプリケーションは、サーバへのログイン情報、アクセスポイントなどのログイン情報や電話番号、パスワード情報などの一連のユーザデータをコマンドとファイルをアダプタ108に送る。コマンドとファイルを受け取ったアダプタ108は、ユーザデータをフラッシュROM3105にブロック書きこみを行う。

【0096】以上の構成において、ユーザデータに関するアダプタ108の動作を説明する。

【0097】通信アダプタが携帯用通信機109を通じてアクセスポイントに接続し、インターネット経由でサーバ（フォトサイト）104と通信するためのデータ（ユーザデータに相当する）を登録しておいて初めて可能になる。アクセスポイントに関する情報の登録機能と、サーバ104に接続するための情報を登録する機能を通信アダプタは持つ。

【0098】（サーバ接続情報登録処理）図6はフォトサイトであるサーバ104に接続するための情報の登録

機能を実現するフローチャートである。

【0099】通信アダプタの108の電源が投入され初期化動作が終わると、通信アダプタ108はデジタルカメラ107の接続を待つ。デジタルカメラ107が接続されると、S3601にてUSBインターフェース処理を行う。ここでは、USBの規格に沿って動作する。この処理のなかで、通信アダプタ108はデジタルカメラの107からの情報（USBのデスクリプタ）を読み出し、そこに含まれるデジタルカメラ107の機種やシリアル番号に相当するカメラID（=CameraID）取得する。また機種確認も行う。

【0100】S3602では不揮発性メモリ保存されているフラグID\_DATAの状態を判定している。このID\_DATAはユーザデータ内にあるカメラID（=CameraID）データの状態を示しセットされているときはSET、いないときはOFFとする。出荷状態ではOFFとなっている。

【0101】カメラID（=CameraID）データがセットされている場合、S3604で先にユーザデータにセットされているカメラID（=CameraID）と今回取得したカメラID（=CameraID）とが一致しているかを判定する。一致しない場合、処理を終える。一致した場合、S3606に進む。

【0102】S3606ではフラグACC\_EnableをONにセットして終了する。このフラグはネットワークに接続するときにユーザデータのデータを使って良いことを示すもので許可するときはON、いないときはOFFとする。なお電源投入時にはこのフラグはOFFとされる。

【0103】S3602にて、通信アダプタ108のユーザデータにカメラ識別子（=CameraID）がセットされていないと判断したときは、S3601で取得したカメラ識別子（=CameraID）をユーザデータに保存し、処理S3306に進む。

【0104】アクセスポイントに関する情報は、PC101を使ってUSB3114経由で設定する。情報の書き込み指示はPCで起動しているプログラムによって行われ、通信アダプタ108がアクセスポイントに発呼するための電話番号、PPP接続のためのログイン名、パスワード等の情報を、PCは通信アダプタ108に転送する。アダプタ108はその情報を記憶する。

【0105】（アクセスポイント接続情報登録処理）図7はアクセスポイント102に関する情報の登録機能を実現するフローチャートである。

【0106】通信アダプタの108の電源が投入され初期化動作が終わると、S3701にて不揮発性メモリ保存されているフラグUserDataを確認する。このUserDataフラグはユーザデータ内にあるアクセスポイントに発呼するための電話番号、PPP接続のためのログイン名、パスワードなどの情報がセットされて

いるかを示すもので、セットされているときはSET、いないときはNotSetとする。出荷状態ではNotSetとなっている。ユーザデータにセットされていると判定した場合、スイッチ操作を待つスタンバイに移行する。

【0107】一方、ユーザデータが書き込まれていないと判定した場合、S3702にてPC101の接続を待つ。アクセスポイントに発呼するための電話番号、PPP接続のためのログイン名、パスワード等の情報をPC101から受けると情報をユーザデータに書き込む。

【0108】S3703ではユーザDataフラグをSet状態にしてスイッチ操作を待つスタンバイに移行する。

【0109】このようにしてPC101はアダプタ108に対してアクセスポイントなどの情報を設定したり読み出したりすることができる。

【0110】（通信処理）図8は通信処理開始の判定を行うフローチャートである。

【0111】イメージデータを送信のためユーザ操作によってボタンが押されるとスタンバイから判断S3801へ進む。判断S3801ではフラグACC\_EnableとUser\_Dataがそれぞれセットされていることを確認している。少なくともいずれか一方がセットされていない場合、何もせず終了する。一方、両フラグともセットされていると判断した場合、すなわち、接続されているデジタルカメラのカメラ識別子と、ユーザデータにセットされているカメラID（=CameraID）とが一致しており、かつ、アクセスポイント関連等の情報もセットされている場合には、通信処理S3802を行い、サーバ通信等を行う。

【0112】フラグACC\_Enableは通信アダプタ108の電源を投入したときにオフに設定されており、その後、接続されたデジタルカメラのカメラIDとアダプタ108の保持するカメラIDとが一致した場合に限ってセットされる。したがって、通信アダプタ108は設定されたデジタルカメラと組でなければ、サーバ104と通信できない。そのため、正当利用者でなければ、通信アダプタを利用できず、不正利用を防止できる。

【0113】図9は通信処理S3802のフローチャートである。ユーザデータにあるカメラID（=CameraID）が同じであり、かつアクセスポイント関連等の情報もセットされているとき、ユーザ情報領域にあるアクセスポイントの番号を使って発呼する（S3901）。アクセスポイント102に接続成功と判断したら（S3902）、ユーザ情報領域に格納されているユーザ名およびパスワードを使ってサーバ（図示せず）に、PPPによってログインする（S3903）。

【0114】発呼、接続、ログインに失敗した場合、通信の規定に従い、リトライする。リトライ回数をオーバ

一した場合は、終了する。

【0115】ログインに成功した場合、HTTPプロトコルにしたがってフォトサイトサーバ104にログインする(S3904)。このときのログイン情報およびパスワードはアダプタ情報領域にあるアダプタIDとユーザ情報領域にあるカメラIDを利用する。ログイン後、同期制御を行い(S3905)、フォトサイトサーバ104からの制御命令を判断する(S3906)。転送許可を受けたら、デジカメより取得した画像データを転送する(S3907)。転送終了後ログアウトし(S3908)、回線を切断する(S3910)。

【0116】以上のように本実施形態の通信アダプタによれば、認識したイメージデバイス(実施形態ではデジタルカメラ)のシリアル番号と記憶している情報とを比較し、不一致のときネットワーク接続を許可しない。このため、通信アダプタをその本来の使用者以外の者が、例えば取得するなどした場合に、フォトサイトであるサーバにより管理されたネットワークシステムへの接続を制限することができる。したがって、紛失・盗難された通信アダプタと登録されていない他の機器との組合せの通信動作を制限することができるので、ネットワークサービス等の不正利用を避けることができる。

【0117】また、イメージデバイスのシリアル番号が登録されているかを判定し、認識したイメージデバイスのシリアル番号を記憶し、発呼を要求するための電話番号、ネットワークに接続するためのユーザ名およびパスワード識別情報等を記憶する。そして、この2つの記憶操作が完了してから通信接続を開始することができるので、むやみに発呼してしまうとか、ネットワークのログインができないといった不具合を解消することができる。さらに登録の手順の信頼性が向上する。

【0118】(第2の実施形態)次に、第2の実施形態を説明する。第2の実施形態の構成は、基本的に第1の実施形態の構成と同じであるので、第2の実施形態の説明では、第1の実施形態の構成を流用する。

【0119】図10は通信処理開始の判定を行うフローチャートである。このフローは先に説明した図8に示す通信処理開始の判定を行うフローチャートに変わるものである。

【0120】イメージデータを送信するためボタンが押されると(ユーザ操作によって)、通信アダプタ108はスタンバイから判断S4001へ進む。ここではフラグUser\_Dataがセットされていることを確認している。セットされていない場合、何もせず終了する。一方判断S4002ではフラグACC\_Enableがオンであるか確認する。不一致の場合、S4003にてUserDataをNotSetにして終了する。

【0121】一方、データが正常と判断した場合、すなわちユーザデータにあるカメラID(=CameraID)が同じであり、かつアクセスポイント関連等の情報

もセットされている場合、通信処理S4004を行い、サーバ通信等を行う。ステップS4004は図9に示した処理と同様の処理である。

【0122】このように、フラグACC\_Enableがオフの場合、ネットワーク通信をさせないばかりでなく、UserDataをNotSetに変更することによって、ユーザデータの更新をさせることができる。ユーザデータの更新は、PC101を用いて図7の手順で行わねばならず、また、交信される内容には、サーバ104に対するログイン名やパスワード等、サーバ104によるサービスの正当利用者でなければ知り得ない情報が含まれていることから、通信アダプタ108の不正利用に対する保護を一層厚くすることができる。

【0123】[その他の実施例] 第2実施形態ではACC\_EnableをOFFの場合、ネットワーク通信をさせないばかりでなく、UserDataをNotSetに変更したが、ユーザデータそのものを消去する方法でも実現できることは言うまでもない。

【0124】第1及び第2実施形態では、デジタルカメラを使ったイメージネットワークサービスを例に説明したが、アダプタとデジタル機器(I/O機器)との組合せで適応できる。特にアダプタとI/O機器が分離でき、モバイル環境で使用する場合に効果がある。

【0125】また、上記各実施形態の構成に代わって、次のような構成を採用するようにしてもよい。すなわち、携帯端末102として、PHS端末やPDC方式(RCRSTD-27)の携帯電話端末を用いても良いし、BluetoothやIEEE802.11規格に従った無線端末を用いることができる。さらに、有線通信を行う固定式電話(モデム)等でも実現できる。

【0126】なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体(または記録媒体)を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ(またはCPUやMPU)が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。

【0127】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体およびプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0128】また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【0129】さらに、記憶媒体から読み出されたプログ

ラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

#### 【0130】

【発明の効果】以上のように本発明によれば次のような効果を奏する。

【0131】接続された周辺装置の識別子が前記第1の記憶手段に記憶された識別子と一致しない場合には、前記ネットワークへの接続を行わず、次のネットワークへの接続に先だって、前記周辺装置の識別子と前記第1の記憶手段に記憶された識別子との照合と、前記第2の記憶手段に記憶された前記接続情報の更新とを行わせることで、正当利用者以外による当該通信制御装置の利用を困難ならしめ、ネットワークサービス等の不正利用を避けることができる。

【0132】さらに、ネットワークへの接続時に必要とされる、接続された周辺装置の識別子が第1の記憶手段により記憶されていない場合には、改めてその照合を行う必要があるために、周辺装置が正当利用者のものでない限り、ネットワークへの不正な接続を制限できる。

【0133】さらに、デジタルカメラ等のイメージデバイスによるネットワークサービスについて、不正利用を防止できる。

【0134】さらに、デジタルカメラ等のイメージデバイスに固有かつ変更不可能な製造番号によりネットワーク接続を制限でき、より不正利用の防止を効果的に行える。

【0135】さらに、接続情報は、ネットワークに接続された情報処理装置から受信する必要があるために、不正利用の防止をより効果的に行える。

#### 【図面の簡単な説明】

【図1】本発明の実施形態を示すシステム構成図である。

【図2】アプリケーションサーバー（104）内のソフトウェアモジュール構成図である。

【図3】本サーバシステムがアダプタ（1020）とデジタルカメラ（1021）に対して提供するサービスと、その各サービスにおいて図2に示したソフトウェアモジュールの呼び出される順序を示したフローチャートである。

【図4】上記実施例におけるアダプタ108の電氣的構成を示すブロック図である。

【図5】FlashROM3105の内部構造示す図である。

【図6】フォトサイトに接続するための情報の登録機能を実現するフローチャートである。

【図7】アクセスポイントに関する情報の登録機能を実現するフローチャートである。

【図8】通信処理開始の判定を行うフローチャートである。

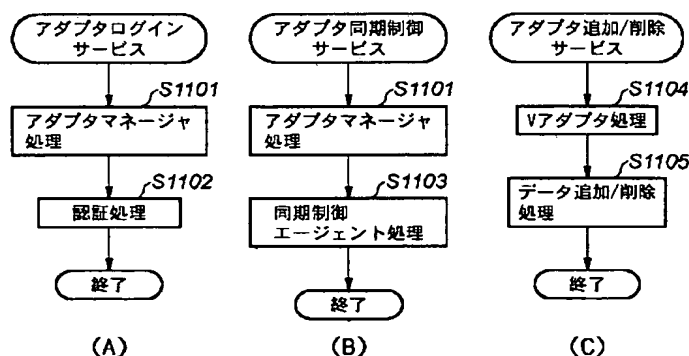
【図9】通信処理S3802のフローチャートである。

【図10】第2実施形態における通信処理開始の判定を行うフローチャートである。

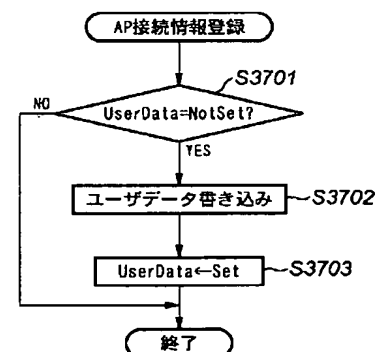
#### 【符号の説明】

- 101 パーソナルコンピュータ（PC）
- 102 アクセスポイント
- 103 インターネット
- 104 フォトサイト
- 105 携帯電話
- 106 ゲートウェイ
- 107 デジタルカメラ
- 108 通信アダプタ
- 109 携帯用通信機
- 110 基地局

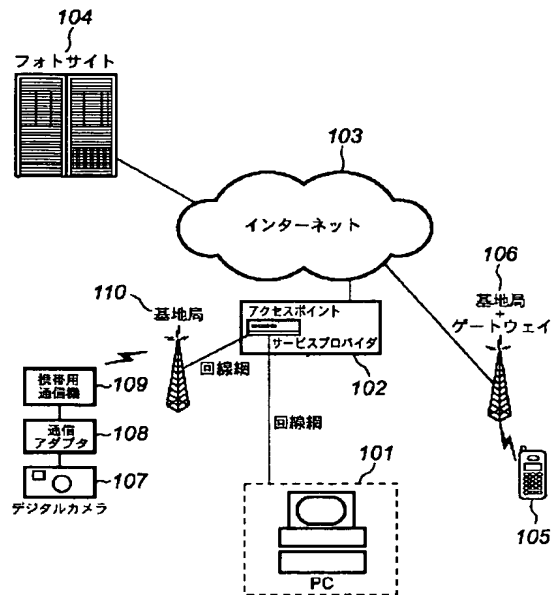
【図3】



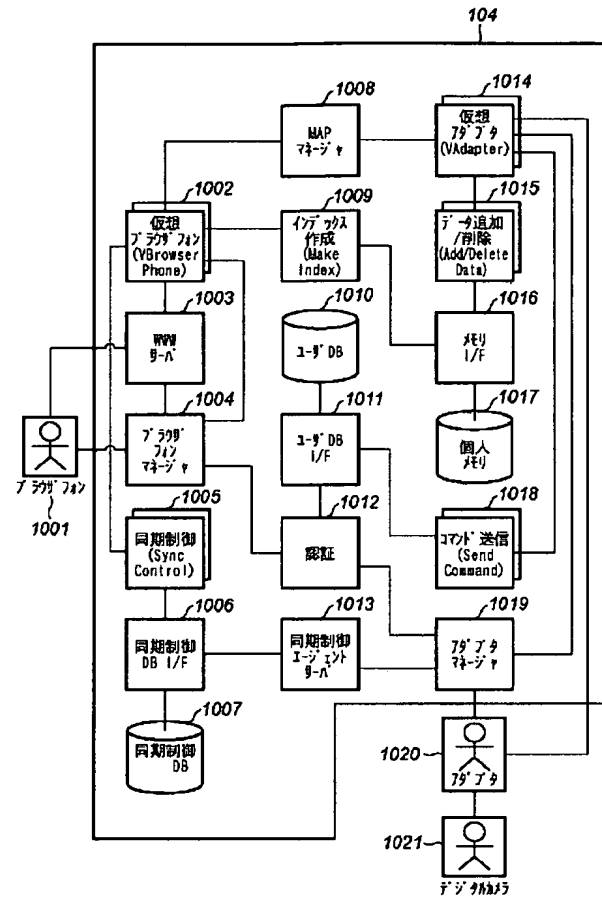
【図7】



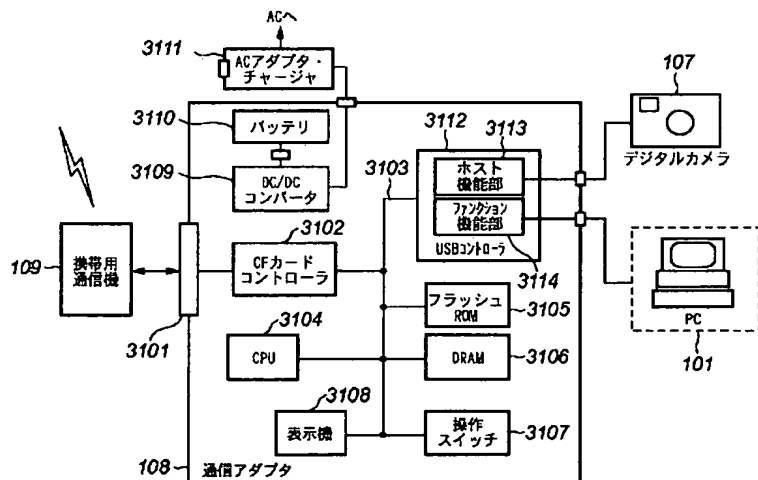
【図1】



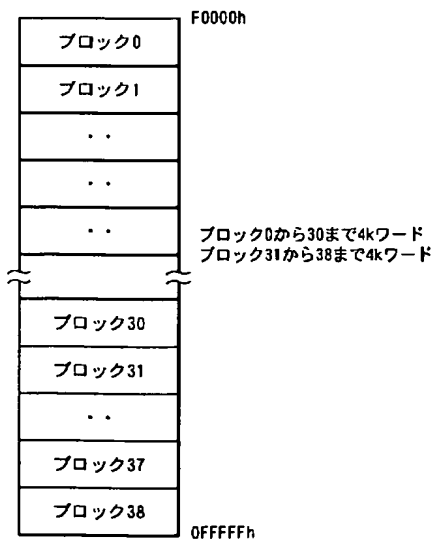
【図2】



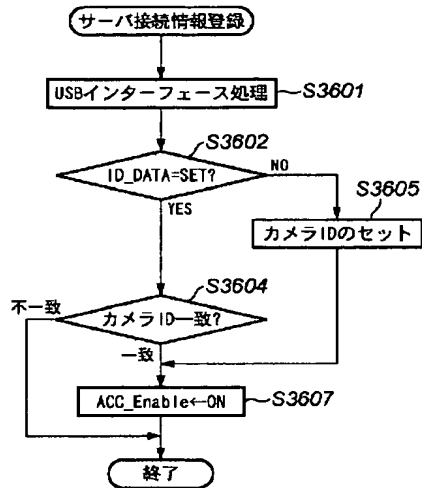
【図4】



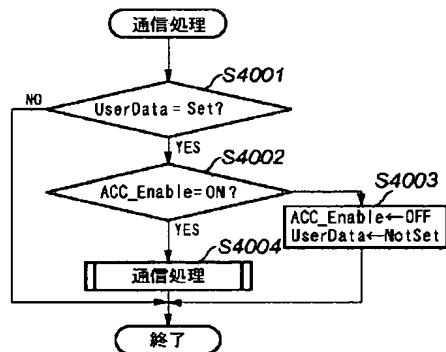
【図5】



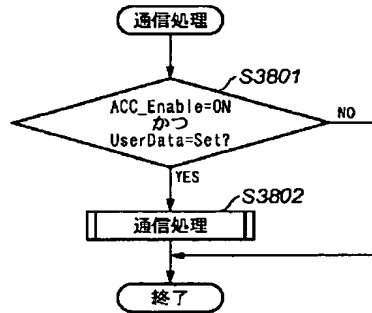
【図6】



【図10】



【図8】



【図9】

